Customer Safety and Abuse Operations

Residential Abuse Ticket Handling Procedures

Revision History

Author	Revision	Date	Notes
Corporate Customer Safety	4.0	10/18/12	

Stakeholders

Department	Represented By
Corporate Customer Safety	CCI-AbuseCorporate@cox.com
Tier 2 NetSec	HRD-.TOC@cox.com

EXHIBIT
CAROthers 3

TABLE OF CONTENTS

Note:

For most Abuse Types (SPAM TROJAN, MALWARE COMP, WEBMAIL COMP, PS MAL-unintentional), the "**Abuse Cycle**" for Cox.net Residential Customers is a **6 month period**. Within this 6 month period, we perform our graduated response procedures (1st Complaint, 2nd, 3rd, WARN/SUSPEND, etc.) upon receiving complaints (Tickets), per each HSI Account. If no complaints related to the previous Abuse Type are received within 6 months from the last complaint, the Abuse Cycle **STARTS OVER**.

When the document states **"Final Suspension"** this means the customer will be talking to the Tier 2 NetSec.
When you speak to a customer on a "Final Suspension" you MUST speak with the account holder, not just any person with the PIN.

When you reactivate a subscriber (or help in general), make sure you are talking to the account holder, an authorized user (ICOMS DE Screen) and they must verify the PIN or Social Security number.
It is prudent to note the CATS Ticket worklog and ICOMS CC notes with the name, contact information and the relation to the Subscriber of the person you are speaking with about the abuse issue.

1.0 Purpose

This is the automated procedure followed by CATS to automatically close tickets.

2.0 Scope

This procedure applies to CATS.

3.0 Process Description

A ticket is automatically assigned the abuse type, AUTO CLOSE, when no criteria for investigation are found in the complaint, such as a Cox IP Address.

4.0 Investigation

Action Items
1. No investigation by a human is necessary

5.0 Resolution

Action Items
1. Auto-closed tickets are handled by CATS and no action by human is necessary
2. Auto-closed tickets are infrequently seen by those working in CATS
3. Occasionally, you might come across a child ticket in which the complainant has responded to the "NO COX IP" auto-reply sent via the auto-closed parent ticket
4. Auto-reply states that the complainant has not provided enough information for abuse@cox.net to conduct an investigation or the matter which they are reporting did not originate from Cox.net
5. This form letter offers suggestions on how to report Internet abuse to the proper authorities
6. If the complainant believes they received the auto-reply in error, they can simply reply to the auto-reply

6.0 References

Document Name	Location
Headers Document	Cox_Communications_Header_Primer.pdf
Manual Suspension Guide	Manual_Suspension_Procedure.pdf

7.0 Definitions, Acronyms, and Abbreviation

Auto Close – Automatically close tickets that do not have a valid Cox IP address

IP Address – Internet Protocol address is a unique address that devices use in order to identify and communicate with each other on a computer network

BANDWIDTH
Data Usage Allowance Education (DUAE)
& Excessive User

1.0 Purpose

This document defines our role in processing reports from DUAE and our responsibility in advising Customers who are considered "Excessive Users".

2.0 Scope

These Procedures apply to Tier 2 NetSec and Corporate Abuse.

3.0 Process Description - DUAE

For DUAE, Abuse/Customer Safety will not be processing these tickets or speaking with the Customers. This initiative is "more of a marketing function", rather than an Abuse process. It will be fully automated. Subscribers will be advised via email only. There will be no suspensions.

4.0 Process Description – Excessive User

Excessive User will be a mostly automated, hard 3-strikes process. It will be automated up to termination. CATS will automatically suspend the Subscriber, for the first two strikes. The 3rd complaint within a 180 day period will result in a 6 month termination.

5.0 Investigation & Resolution

Action Items
You've encountered an open CATS Ticket for Abuse Type **BANDWIDTH…**
1. If the complaint is for ***DUAE***, promptly notify CCIATL-DataOps-CATS@cox.com & CC: CCI-AbuseCorporate@cox.com
2. If the complaint is for ***Excessive User***, this should be the "3rd Strike" and the ticket for which the Subscriber's termination will be performed & documented.

6.0 General Guidelines

1. DUAE tickets should be fully automated. Any BANDWIDTH – DUAE tickets left open by CATS should be brought to the attention of the CATS Administrator - CCIATL-DataOps-CATS@cox.com
2. Subscribers terminated for BANDWIDTH – Excessive User will have a termination period of no less than 6 months.

7.0 References

Document Name	Location
KIQ Article?	?
BANDWIDTH / Excessive User Walled Garden page?	?

8.0 Definitions, Acronyms, and Abbreviation

DUAE – Data Usage Allowance Education; a process for educating Customers about the amount of bandwidth they are using.

Excessive User – a Subscriber who is grossly abusing their bandwidth limitations, using 2X or more than their allotted bandwidth, within a single billing cycle.

BLACKLIST

1.0 Purpose

This section defines steps for handling complaints from Customers or 3rd parties who believe that their emails are being blacklisted by Cox or a 3rd party, such as SORBS, Spamhaus, CBL, etc.

2.0 Scope

These Procedures apply to Tier 2 NetSec and Corporate Abuse.

3.0 Process Description

Abuse@Cox.net may occasionally receive complaints from non-Cox.net Subscribers that their emails are being blocked by Cox. We may also receive complaints from Cox.net Subscribers about our mail servers being blacklisted by a 3rd party and they are unable to send emails to a particular contact at another ISP or organization. For these complaints, we should set the Abuse Type to BLACKLIST.

4.0 Investigation

Action Items
1. Read the complaint and determine whether the party blacklisted is a Cox.net Subscriber or a 3rd party.
2. Examine the complainant's headers above the complaint.

5.0 Resolution – 3rd Party Complainant

Action Items	
1. If it is a non-Cox Customer reporting the issue:	Reply and send the "Blacklist (Reply to External Party)" Form Letter.

6.0 Resolution – 3rd Party Complainant

Action Items	
1. If it is a Cox.net Customer reporting the issue:	1. Reply and send the "Blacklist Reply to CUST 2" Form Letter.
	2. Notify Corporate Abuse – cci-abusecorporate@cox.com – of the complaint and provide the details.
	3. Await any response from the Subscriber and share any additional information with Corporate Abuse – cci-abusecorporate@cox.com

7.0 General Guidelines

Action Items
1. If the request is not clear, you can send a response to the complainant requesting additional information.
2. If you are unsure of the appropriate course of action, reach out to Corporate Abuse – cci-abusecorporate@cox.com
3. The Postmaster Page has helpful information - http://postmaster.cox.net

8.0 References

Document Name	Location
Headers Document	Cox_Communications_Header_Primer.pdf
Cox.net Postmaster Page	http://postmaster.cox.net
MX Toolbox Blacklist Check	http://www.mxtoolbox.com/blacklists.aspx

9.0 Definitions, Acronyms, and Abbreviation

Email Blacklist – An email blacklist blocks email considered spam. unsolicited emails sent via an automatic system from entering recipients' email inboxes.

Email Filter – Most often this refers to the automatic processing of incoming messages, but the term also applies to the intervention of human intelligence in addition to anti-spam techniques, and to outgoing emails as well as those being received.

COPYOTHER

1.0 Purpose

These procedures define the steps in responding to Copyright Infringement Take-down Notices

2.0 Scope

These procedures apply to Tier 2 NetSec and Corporate Abuse.

3.0 Process Description

Subscribers may not use their Cox Internet Services to post, copy, transmit, or disseminate any content that infringes the patents, copyrights, trade secrets, trademarks, or propriety rights of any party.

Our policy states that each case will be reviewed individually before termination. Please convey to our Subscribers that, depending upon the circumstances, if we continue to receive notices of their infringement, their service may be suspended and/or terminated.

Action Items

4.0 Investigation

Action Items	
1. Verify that the notice(s) in the ticket is/are valid. A valid DMCA Notice should contain the following: A. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. 1. PGP signatures are required for automation 2. "signed…" & "/s/" are accepted as signatures B. Identification of the copyrighted content claimed to have been infringed. C. The location (IP Address, Port, URL, etc) of the infringing content. D. The complainant's contact information. E. Statement of "good faith belief" F. Statement of "under penalty of perjury"	
2. If the notice is missing any of the above requirements or if there is an error for the PGP signature	Notify CCI – Abuse Corporate, providing Ticket #
3. Verify that the correct Subscriber was identified by checking the infringement date & time and compare it with CATS DHCP Records. Update the ticket with the correct Subscriber or Abuse Date, if required.	

5.0 Resolution – First Offense

Action Items	
1. For the First Offense, within a 6 month period.	*"Hold for further complaints."*

6.0 Resolution – Repeated Offenses *with* Preferred or Cox.net Email Contact Available

2nd Offense	Send Email Warning
3rd	Send Email Warning
4th	Send Email Warning
5th	Send Email Warning
6th	Send Email Warning
7th	Send Email Warning
8th	Suspend Customer has option to self-reactivate
9th	Suspend Customer has option to self-reactivate
10th	Suspend to Tier 2 800#. Provide Tier 2 Worklog Notes
11th	Suspend to Tier 2 800#. Provide Tier 2 Worklog Notes
12th	Suspend to Atlanta 404# Advise Subscriber that if we continue to receive complaints, after this suspension, their account will be under review for termination.
13th	Suspend to Atlanta 404# Advise the Subscriber that their account is under review for termination by and it may take up to several business days to complete the review.
Continued Offenses	Suspend to Atlanta 404# Account will be reviewed and considered for termination.
Action Items	

7.0 Resolution – Repeated Offenses – *without* Preferred or Cox.net Email Contact Available

Action Items	
2nd Offense	Suspend Customer has option to self-reactivate
3rd	Suspend Customer has option to self-reactivate
4th	Suspend to Tier 2 800#. Provide Tier 2 Worklog Notes
5th	Suspend to Tier 2 800#. Provide Tier 2 Worklog Notes
6th	Suspend to Atlanta 404# Advise Subscriber that if we continue to receive complaints, after this suspension, their account will be under review for termination.
7th	Suspend to Atlanta 404# Advise the Subscriber that their account is under review for termination by and it may take up to several business days to complete the review.
Continued Offenses	Suspend to Atlanta 404# Account will be reviewed and considered for termination.

8.0 General Guidelines

Action Items

1. Check if Subscriber may be operating an unencrypted / open wireless network.
2. Advise Subscriber to check all systems connected to their network for Peer to Peer file-sharing applications - *Torrent, Limewire, Kazaa, eDonkey, etc.

9.0 References

Document Name	Location
General information & FAQs about DMCA notices	http://www.respectcopyrights.org/
DMCA Walled Garden	http://abuse-sb1.corp.cox.com/template/dmca

10.0 Definitions, Acronyms, and Abbreviation

Copyright – is the set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work.
DMCA – Digital Millennium Copyright Act is a United States copyright law which criminalizes production and dissemination of technology that can circumvent measures taken to protect copyright

AV – Antivirus (or "anti-virus") software is program that searches your hard drive and floppy disks for any known or potential viruses

DENIAL OF SERVICE

1.0 Purpose

This procedure defines steps for responding to DoS complaints.

2.0 Scope

These Procedures apply to Tier 2 NetSec and Corporate Abuse.

3.0 Process Description

Denial of Service is an attempt to make a computer resource unavailable to its intended users.

A Distributed Denial-of-Service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of